Zadania kwalifikacyjne

1 Wstęp

Rozwiązania zadań proszę wysyłać na adres mieszko1037@gmail.com do końca maja z tematem "Warsztaty WWW [Imię i nazwisko]". Gorąco zachęcam jednak do wysyłania ich wcześniej - wyślę wtedy wiadomość zwrotną z informacjami o błędach, jeżeli jakieś znajdę i podpowiedziami. Rozwiązania przyjmuję w dowolnej postaci - najwygodniejszy byłby LaTeX, ale mogą być nawet zdjęcia odręcznych notatek - byleby czytelne. Nie trzeba oczywiście zrobić w zupełności wszystkich zadań. Warto wysyłać nawet częściowe pomysły do niektórych, wezmę je pod uwagę przy ocenianiu. W razie jakichkolwiek wątpliwości, niezrozumienia treści, oznaczeń itp. - też piszcie.

2 Grupy

Niech X będzie dowolnym zbiorem. Działaniem dwuargumentowym na X nazywamy dowolną funkcję $f : X \times X \to X$. Jest to więc przyporządkowanie każdym dwóm elementom zbioru trzeciego - wyniku działania. Zwykle będziemy pisali afb zamiast $f(a, b)$. Jest to powszechnie przyjęta konwencja - dodając liczby rzeczywiste każdy z nas pisze raczej $x + y$ zamiast $+(x, y)$. Możemy teraz wprowadzić fundamentalną dla całej algebry definicję.

Grupą nazywamy parę $(G, \Diamond)$, gdzie G jest niepustym zbiorem, a $\Diamond$ działaniem dwuargumentowym na tym zbiorze, spełniającym następujące warunki:

- dla każdych $a, b, c \in G : \ (a\Diamond b)\Diamond c = a\Diamond(b\Diamond c)$ (nazywamy to łącznością działania $\Diamond$);
- istnieje $e \in G$ taki, że dla każdego $a \in G : \ a\Diamond e = e\Diamond a = a$ (element e nazywamy elementem neutralnym grupy);
- dla każdego $a \in G$ istnieje $b \in G$ taki, że $a\Diamond b = b\Diamond a = e$ (element b nazywamy elementem odwrotnym do a).

Jeżeli dodatkowo zachodzi warunek

- dla każdych $a, b \in G : \ a\Diamond b = b\Diamond a$

to grupę nazywamy przemienną lub abelową.

Klasycznymi przykładami są liczby rzeczywiste z dodawaniem, liczby rzeczywiste dodatnie z mnożeniem, liczby wymierne z dodawaniem itp.

1. Sprawdź, czy poniższe struktury są grupami:

   (a) $(\mathbb{Z}, +)$, gdzie $+$ jest zwykłym dodawaniem

   (b) $(\mathbb{R}, \times)$, gdzie $\times$ jest zwykłym mnożeniem

   (c) $(\mathbb{R} \setminus \{0\}, \times)$

   (d) $(\mathbb{Z}_p^*, \times_p)$, gdzie p jest liczbą pierwszą, $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$ i $a \times_p b = (ab)\ mod\ p$, czyli reszta z dzielenia iloczynu ab przez p

2. Udowodnij, że w każdej grupie istnieje dokładnie jeden element neutralny.

3. Udowodnij, że w każdej grupie dla każdego elementu istnieje dokładnie jeden element odwrotny.

4. Udowodnij, że jeżeli $(\{a_1, a_2, ..., a_n\}, \Diamond)$ jest skończoną grupą abelową, to

$$a_1 \Diamond a_2 \Diamond ... \Diamond a_n = b_1 \Diamond b_2 \Diamond ... \Diamond b_k$$

   gdzie $B = \{b_1, b_2, ..., b_k\}$ jest zbiorem wszystkich elementów G o tej własności, że $b_i \Diamond b_i = e$ (zauważ, że zbiór ten jest zawsze niepusty, bo $e \in B$).

5. Wywnioskuj z powyższego zadania twierdzenie Wilsona:
   Liczba naturalna $p > 1$ jest pierwsza wtedy i tylko wtedy, gdy

$$p \mid [(p-1)! + 1]$$

3 Ciała

Grupa jest przykładem struktury zbioru z jednym działaniem o bardzo dobrych własnościach. W praktyce mamy jednak często do czynienia ze zbiorami, na których określone są dwa działania, które są ponadto ze sobą powiązane (np. $(\mathbb{R}, +, \times)$). Sensownym uogólnieniem takich struktur jest pojęcie ciała.

Ciałem nazywamy trójkę $(K, +_K, \times_K)$, gdzie K jest niepustym zbiorem, a $+_K$ i $\times_K$ są działaniami dwuargumentowymi na K spełniającymi następujące własności:

- $(K, +_K)$ jest grupą abelową;
- $(K \setminus \{0_K\}, \times_K)$ jest grupą abelową, gdzie 0_K jest elementem neutralnym grupy $(K, +_K)$;
- dla każdych $a, b, c \in K:\ a \times_K (b +_K c) = (a \times_K b) +_K (a \times_K c)$.

Działania $+_K$ i $\times_K$ często nazywamy po prostu dodawaniem i mnożeniem w ciele K. Element neutralny $(K \setminus \{0_K\}, \times_K)$ oznaczamy zwykle przez 1_K i nazywamy jedynką ciała K, a element 0_K - zerem ciała K.

1. Udowodnij, że dla każdego ciała K i dla każdego $a \in K$ zachodzi $a \times_K 0_K = 0_K \times_K a = 0_K$.
2. Sprawdź, czy $(\mathbb{Q}(\sqrt{3}), +, \times)$ jest ciałem, gdzie $\mathbb{Q}(\sqrt{3}) = \{p + q\sqrt{3} : p, q \in \mathbb{Q}\}$, a + i × są zwykłym dodawaniem i mnożeniem.

4 Przestrzenie liniowe

Przestrzenią liniową nad ciałem K nazywamy zbior V (jego elementy nazywamy wektorami) z działaniami $+ : V \times V \to V$ oraz $\times : K \times V \to V$ nazywami odpowiednio dodawaniem wektorów oraz mnożeniem wektora przez skalar, które spełniają następujące własności:

- $(V, +)$ jest grupą abelową;
- dla każdych $a \in K, v, w \in V :\ a \times (v + w) = a \times v + a \times w$;
- dla każdych $a, b \in K, v \in V :\ (a + b) \times v = a \times v + b \times v$;
- dla każdych $a, b \in K, v \in V :\ a \times (b \times v) = (a \times_K b) \times v$;
- dla każdego $v \in V :\ 1_K \times v = v$.

Ta definicja jest bardzo abstrakcyjna i bardzo ciężka w użyciu. Na szczęścia mamy twierdzenie, które pozwala nam opisać przestrzenie liniowe w dużo prostszy sposób:

W każdej przestrzeni liniowej istnieje baza, tzn. podzbiór B zbioru V taki, że każdy element $v \in V$ może być zapisany w postaci $v = a_1 \times b_1 + ... + a_k \times b_k$, gdzie $a_i \in K \setminus \{0\}, b_i \in B$ i to na dokładnie jeden sposób. Co więcej, każde dwie bazy są równoliczne.

W przypadku, gdy baza jest skończona, ma, powiedzmy, n elementów, możemy przyporządkować każdego wektorowi $v \in V$ pewien element $(a_1, a_2, ..., a_n) \in K^n = K \times K \times ... \times K$. Liczbę n nazywamy wówczas wymiarem V nad K. Widzimy, że istnieje zachowująca działania bijekcja (tzw. izomorfizm) pomiędzy $(V, +_V, \times_V)$ i $(K^n, +, \times)$, gdzie + jest zwykłym dodawaniem "po współrzędnych", a × jest zwykłym mnożeniem przez każdą współrzędną z osobna. Typowymi przykładami są $\mathbb{R}^2$ nad $\mathbb{R}$ utożsamiana z płaszczyzną i $\mathbb{R}^3$ nad $\mathbb{R}$ utożsamiana z przstrzenią trójwymiarową.

1. Czy zbiór wielomianów jednej zmiennej o współczynnikach rzeczywistych stopnia co najwyżej 5 jest przestrzenią liniową nad $\mathbb{R}$? Jeżeli tak, to wyznacz jej wymiar i wskaż bazę.